DAHLGREN DIVISION
NAVAL SURFACE WARFARE CENTER
Dahlgren, Virginia 22448-5100

NSWCDD/TR-01/16

QUALIFYING RISK: MISSION READY CERTIFICATION OF SHIPBOARD SYSTEMS

BY RICHARD A. HOLDEN

COMBAT SYSTEMS DEPARTMENT

JULY 2001

REPORT DOCUMENTATION PAGE	Form Approved OMB No. 0704-0188

1. AGENCY USE ONLY (Leave blank)	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	July 2001	Final

4. TITLE AND SUBTITLE

QUALIFYING RISK: MISSION READY CERTIFICATION OF SHIPBOARD SYSTEMS

5. FUNDING NUMBERS

6. AUTHOR(s)

Richard A. Holden

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Commander
Naval Surface Warfare Center
Dahlgren Division (Code N10)
17320 Dahlgren Road
Dahlgren, VA 22448-5100

8. PERFORMING ORGANIZATION REPORT NUMBER

NSWCDD/TR-01/16

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION/AVAILABILITY STATEMENT

Approved for public release; distribution is unlimited.

12b. DISTRIBUTION CODE

A

13. ABSTRACT (Maximum 200 words)

This report documents the results of a series of studies of the impact of Acquisition Reform on the process of engineering systems used aboard ships during operational deployments and, specifically, the impact on the engineering process if commercial items are used in place of the traditional uniquely Navy products. An input-output model is used to represent the core technical process of developing, producing, and supporting shipboard systems. A basis of this core technical process is certifying systems as mission ready, that is, available, reliable, and maintainable over their life cycles. The foundation of system certification is qualifying risk to the users who must depend on the systems to work as expected. Certification of commercially based military systems can be accomplished by a disciplined engineering and management infrastructure. Overcoming acquisition and legislative roadblocks is critical, and organizational changes are required within the naval shore establishment to create an infrastructure that can accept absolute responsibility and be accountable for ensuring that the material elements of deploying commands are mission ready.

14. SUBJECT TERMS

Acquisition Reform, software, development, system engineering, warships, shipboard systems, commercial off-the-shelf, COTS, certification, mission, readiness, risk, standards, quality assurance, legislation, US Code

15. NUMBER OF PAGES

52

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED	UL

NSN 7540-01-280-5500

Standard Form 298 (Rev 2-89)
Prescribed by ANSI std. Z39-18
298-102

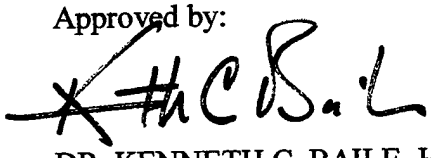
FOREWORD

This report documents work conducted by the Surface Ship and Combat Systems Engineering Division (N10) of the Combat Systems Department (N). It was initiated at the request of Dr. Thomas Clare, former Executive Director of the Naval Surface Warfare Center, Dahlgren Division (NSWCDD), and completed as directed by Dr. Kenneth Baile, Head, Combat Systems Department.

The author acknowledges the contributions of others at NSWCDD to this work.

- In general, those who participated in the initial phases of the study and in the Non-developmental Item/Commercial Off-the-Shelf (NDI/COTS) Workshop in October 1996 for bounding the scope of the study.
- In particular: Mr Reuben Pitts, Surface Ship Program Office, for stimulating discussions that helped to solidify the report and the nine implicit factors of certification listed in Section 6; James B. Bechtel, Esq. Patent Counsel, for review and valuable suggestions for Section 7; and Mr. Jose Gonzalez, Command & Combat Control Systems Division Engineer, for numerous discussions throughout the life of the study.
- And most importantly, Captain Vaughn Mahaffey, USN, former Commanding Officer of the Naval Surface Warfare Center, Dahlgren Division, for support and encouragement during the initial portion of the study.

Approved by:



DR. KENNETH C. BAILE, Head
Combat Systems Department

CONTENTS

ILLUSTRATIONS

TABLES

EXECUTIVE SUMMARY

This report documents the results of a series of studies of the impact of Acquisition Reform on the process of engineering systems used aboard ships during operational deployments. The initial study focused on the question: What role should the in-house naval engineering community play in acquiring and supporting future systems, and specifically, what is the impact on the engineering process if commercial products are used versus the traditional Navy products? Subsequence studies investigated various aspects of this compound question.

A fundamental feature of the traditional acquisition process was product ***certification***; that is, the risk to the user was known, understood, and minimized. This concept of certification carries with it both legislative and engineering responsibility. Certifying a system means ***qualifying*** the ***risk*** in using it by:

- Defining risk criteria.
- Verifying the system meets the definition.
- Testifying to the fidelity of the verification.

Certifying shipboard systems is an integral part of acquisition. The ashore engineering and management infrastructure is accountable for ensuring that the material elements of a deployed command are ***mission ready***. To be mission ready, shipboard systems must be available, reliable, and maintainable over their life cycle. Certification reflects knowledge of the system design and how it is maintained. The act of certification implicitly states that:

- The intended use of the system is understood.
- The environment the system will operate in is known.
- The system design is consistent with the operating environment and intended use.
- The system was implemented consistent with its design.
- The capabilities and limitations of the system implementation are known.
- The maintenance process will preserve the design implementation.
- Design changes (even the most minor ones) will require recertification.
- The system was properly installed aboard ship.
- The ship's crew has correct and sufficient information to operate and maintain the system at sea.

The fundamental concept of developing, producing, and supporting shipboard systems is represented by an input-output model of the core technical process for engineering and management of military systems. Inputs to the process are derived from policy, mission needs, and resources and the outputs of the process are products to be used by the operational maritime force. Acquisition Reform has introduced important changes in the input to the core technical process for shipboard systems, particularly for weapons that contain computer controlled fire

control loops. These changes have destabilized the process for some shipboard systems in terms of qualifying their risk to the user and certifying them as mission ready. To reconstitute a stable, cost effective process, it is necessary to understand system certification in terms of the core technical process and the changes in input introduced by Acquisition Reform. There are organizational and acquisition roadblocks to a smooth transition to a new core technical process.

Overcoming organizational roadblocks requires dealing aggressively with commercial products that have short lifetimes by:

- Integrating the roles of development, production, and support.
- Creating buffers to rapid changes and the obsolescence of commercial items.

In addition, nondisclosure of information about proprietary commercial products is a special problem in establishing a new core technical process. Nondisclosure and short lifetime issues form interrelated roadblocks to acquisition, and overcoming one may help overcome the other. And, both are roadblocks to qualifying risk and ultimately certifying systems as mission ready. Alternative methods for government use and protection of proprietary products are needed, and one approach could involve establishing a second source for selected commercial products. Institutionalizing a new core technical process involves management, engineering, and legislative issues. Consideration should be given to review and possible modification of the United States Code and the DoD acquisition instructions based upon it.

The study reported here is not all encompassing. Not addressed are systems used ashore for such purposes as simulation, analysis, or training. Nor is the use of commercial products in hull and machinery systems considered. The issue of electromagnetic interference is not included although it is a growing problem due to the increased use of communication equipment aboard ship. Although standards are necessary for certification, this study did not review the residual Military Standards and available commercial standards. Work following this study should address certification at the total ship level and encompass hull, machinery, weapons, and communications.

1.0 INTRODUCTION

This report documents a series of studies that were done to assess the impact of Acquisition Reform on the process of engineering systems used aboard ships during operational deployments. Acquisition Reform advocates using commercial products and "managing the suppliers not the supplies." This new approach raises a complicated question: What should be the role of the in-house naval engineering community in acquiring and supporting future systems, and specifically, what is the impact on the engineering process if commercial products are used in place of traditional Navy products?

The challenge in answering this complicated question was to unravel the interrelationship of organization, process, and product to identify those characteristics that must be preserved in going from the old traditional approach to the new Acquisition Reform approach. There were many differences that arose in comparing the old with the new, and each of these differences was perceived at one time or another to be ***the*** issue in using commercial products. Differences in approach involved almost everything that characterized process and product; for example, configuration management, hardness, maintenance, interfaces, security, performance, testing, requirements, and documentation. Identifying differences as issues only succeeded in causing the proponents of Acquisition Reform to view the results as complaints about change and a desire to continue the status quo. This criticism led to focusing on why, in the traditional approach, things had been done the way they had. Was there an underlying motive, or was it simply a way to create jobs and bureaucracy? It was concluded that, although there was ample bureaucracy surrounding it, there was an underlying motive for the traditional process. And that motive was to ensure products would work as expected when used under military conditions.

A singular example of the desire that products work as expected under military conditions occurred during the Normandy invasion June 6, 1944. Receiving news that the invasion was on, several American factories momentarily shut down assembly lines so the workers could pray that the equipment they had supplied would not fail the Allied troops who were perceived at that moment to be engaged in combat. Since 1944 some military products have grown into complex computer controlled systems. However, the desire that military systems not fail those who depend on them has not changed, nor can it change. Satisfying this desire was the underlying motive and the legacy of the traditional acquisition process. The results of the series of studies reported here have identified this fundamental feature of the traditional acquisition process as ***certification***; that is, the risk to the user is known, understood, and minimized. This concept of certification carries with it both legislative and engineering responsibility. The government is ultimately responsible to its people for the actions of military commanders and for the systems they use. Certifying shipboard systems is an integral part of acquiring them, and the management and engineering infrastructure is accountable for ensuring that the material

elements of an afloat command are ***mission ready***—available, reliable, and maintainable. Although factory workers in private industry may never again need to pray that their products not fail the troops, it will always remain the responsibility of the government to establish and maintain an infrastructure to ensure that the risks of such failures are minimized.

The studies reported here considered the impact of Acquisition Reform on engineering Navy systems intended for deployment at sea. Systems used ashore for other purpose such as simulation, analysis, or training were not specifically considered. Other studies have been conducted on the qualification of shore based acquisition support systems [1]. And the Joint Chiefs of Staff have assumed the responsibility for interoperability requirements certification [2].

This report describes two approaches to engineering complex, automated weapon systems:

- The traditional approach using Navy qualified components, and
- The Acquisition Reform approach using components commercially available off-the-shelf.

Both these approaches may be regarded as extreme. The traditional approach adapted to an environment in which the applicable technologies were developed and controlled by the Department of Defense. When this control was made impossible by the rapid growth of digital technology in the commercial market, a change in process was needed. The traditional approach had been successfully used for decades, but its layered bureaucracy could not easily purge unnecessary and outdated elements of the process, and it evolved at its own rate, not in response to the competitive commercial market. In contrast, the reform approach, in use for less than a decade and untested for large complex systems, avoids the ponderous military acquisition process and depends on products that are developed rapidly in response to the competitive commercial market. The reform approach assumes commercial products can be readily used as unmodified parts of military systems.

These two approaches—one slow, plodding, and methodical; the other fast, adaptable, and entrepreneurial—have a common purpose; to produce complex shipboard systems that work as expected and can be supported at sea. The remainder of this report provides results of studies conducted off-and-on from 1995 through 2000 to investigate the basic process of providing and supporting shipboard systems.

2.0 THE CORE TECHNICAL PROCESS

The fundamental concept for developing, producing, and supporting shipboard systems is the input-output model that represents the core technical process for engineering military systems as shown in Figure 1. Inputs to the process are derived from policy, mission needs, and resources, and the outputs of the process are products to be used by the operational maritime force. Where:

- **Policy** is the result of legislation that is expressed in the United States Code and also interpreted by instructions issued by the Office of Secretary of Defense, the Office of the Secretary of the Navy, and the Chief of Naval Operations. Policy can include priority and cost.
- **Mission needs** are derived from national and international policy and from operational experiences of deployed forces and can include operational performance and schedule.
- **Resources** include funding, manpower levels, and regulatory power.
- **Products** are certified shipboard systems and all that goes with them, such as documentation, expendables, and spare parts.

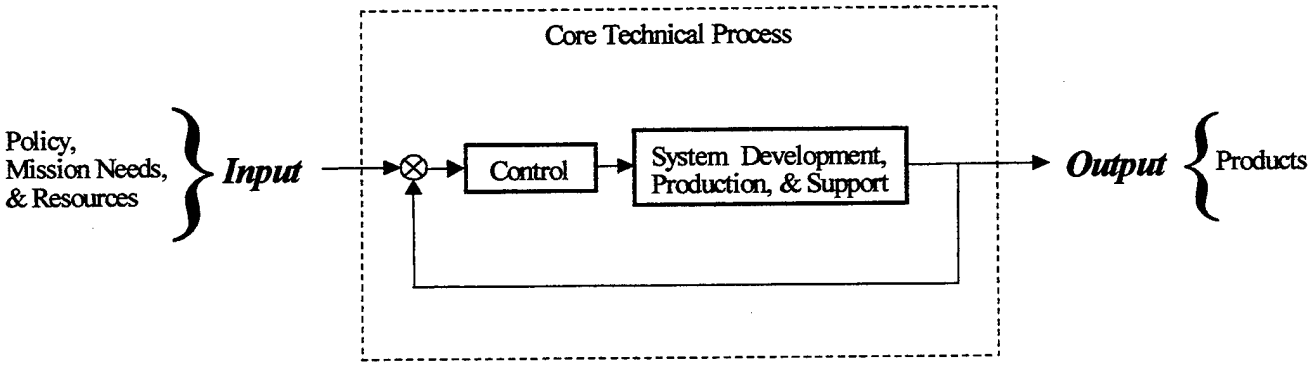


FIGURE 1. INPUT-OUTPUT MODEL

The core technical process is not self supporting, it is sustained by input resources. The primary purpose of the process is to provide the desired output, and ideally, this should be done with the least amount of resource input. The cost of operating the process is determined by the process itself, not by limiting input resources.

In Figure 1, input is converted to output by the core technical process. Ideally the process is linear and stable; that is, the output is proportional to the input for a wide range of inputs. The

process will have an input-to-output response time that determines the interval between the desire for a product and delivery of the product. Response time will depend on inputs and on the process itself. Ideally the process is designed so that the time required to fill a need is minimized. Response time is an inherent characteristic of the process and it cannot be changed simply by changing the rate of change of the input.

The actual process represented in Figure 1 is a complex of interrelated government and industry organizations and facilities, and there are multiple inputs and outputs at different points within the complex. Arbitrary changes can occur in the inputs inducing variance that can cause the process response to become nonlinear or unstable. Instability is reflected by products that are inadequate, too expensive, or appear too slowly. When this occurs, the core technical process will adapt, if possible, and a modified process emerge that is responsive, linear, stable, and cost effective. Adaptation typically involves a learned tinkering with the controls to change the process to the desired behavior. Acquisition Reform has introduced important changes in the input to the core technical process for shipboard systems, particularly for weapons that contain computer controlled fire control loops. These changes have destabilized the process for some shipboard systems in terms of qualifying their risk to the user and certifying them as mission ready. To reconstitute a stable, cost effective process, it is necessary to understand system certification in terms of the core technical process and changes in input introduced by Acquisition Reform.

2.1 ACQUISITION REFORM AND SYSTEM CERTIFICATION

By the early 1990s the basic motive of the tradition acquisition process—quality control—had become buried under years of acquisition process evolution and, to proponents of reform, the only visible characteristics of engineering military systems were expense, inefficiency, and bureaucracy.* This perception was intensified by revolutionary changes in office automation and personal communications brought about by the widespread use of digital computers. Digital technology developed by the Department of Defense in earlier decades had been slowly transferred to private industry and, by the 1980s, inexpensive commercial computers were readily available. The Navy standard computer, the AN/UYK-43, that was deployed on newly constructed ships starting in 1983 was, in terms of processor speed and memory, less capable than commercial computers that were selling daily for a few hundred dollars. To the advocates of reform, the traditional process was a roadblock to acquiring the latest technology inexpensively from commercial vendors [3]. Indeed, a commercial computer with more than ten times the speed and memory could be bought over-the-counter for less than one tenth the cost of the AN/UYK-43. Acquisition comparisons were usually limited to speed, memory, and cost, and the concepts of quality assurance and certification were not visible. The end of the Cold War with the Soviet Union offered an opportunity for reform. With the threat of war ended, reform could be experimented with in a peacetime environment where a new core technical process based on commercial products could be evolved in relative military security.

* The General Accounting Office has declared that the quality assurance goal is "...to ensure products perform the way they are supposed to..." and perceived the DoD's quality assurance practices as adding unnecessary overhead (letter report, 08/26/96, GAO/NSIAD-96-162).

Examples used to support the Acquisition Reform movement are typically based on the procurement of non system products such as ant bait or chairs, or, for example, comparisons of personal computer speed and memory with military system components such as the AN/UYK-43. In these comparisons, the traditional military approach is shown to be far more costly than the commercial or private approach. These comparisons are true, the costs are radically different, and the traditional acquisition process has likely been inefficient in acquiring products. The Department of Defense process for acquiring ant bait, chairs, and other expendable and non expendable commercially available products may indeed be streamlined and a real cost savings realized. Unfortunately, comparisons are limited to such simple products and the process for acquiring complex military systems such as a surface combatant has no equivalent counterpart in the private sector. "Systems" are typically two or more physically and functionally related parts that are interconnected to form a "machine" capable of converting input to output. Computer controlled systems have the added complexity of a computer program* that executes in real time to automatically operate the machine.

Comparison of military weapon systems with commercial systems can be made to a degree. The typical examples given are banking and automated chemical plants.

- Banking and weapons are argued to be similar in that failure of either while in use will result in financial loss. Banking systems are designed for the accurate transfer and accounting of money. Weapon systems are designed to destroy property and take human life. The destruction of property and life in combat does not compare one-for-one with money lost in a faulty financial transaction.
- Automated chemical plants, like automated weapons, could malfunction and cause fire or explosion and the destruction of the plant/weapon itself. There is a greater parallel here than with banking. However, chemical plants are not designed to destroy and kill; they are designed to be cost effective and safely and accurately process products from raw materials.

These examples illustrate two points. Weapon systems have some features in common with automated commercial systems such as banking and chemical plants, but their purpose is radically different. Design and purpose are not easily separated, and design differences must be taken into account. Additional criteria apply to the procurement of weapons. Failure of a system in combat cannot be recovered by suing the vendor who sold the faulty product, or arresting and jailing the hacker who sent the system awry. A malfunctioning banking system or chemical plant can be shut down or taken off-line, creating only a temporary inconvenience to the customer until it is properly working again. A system that malfunctions in combat requires an entirely different response from its operators and can result in far more than an inconvenience to those depending upon it.

An additional difference in commercial and military systems is the concept of "battleshort." That is, the capability to continue operation, or start operation, despite equipment status anomalies that would otherwise render the equipment unavailable. Battleshort bypasses safety

* Throughout this report the term "computer program" means executable code in the form of firmware and software stored in a readable media. The term "software" is used to mean all other forms of software including source code.

interlocks and equipment protective devices except those whose bypassing would cause immediate and serious casualty in the event of a fault condition. Battleshort is an abnormal mode of operation used in emergencies and is a design feature of selected systems. In essence, battleshort provides the option of allowing a system to potentially incur limited damage to prevent a greater loss.

Acquisition Reform advocates the use of commercial products in military systems to the maximum extent possible. The consumer marketplace is such that producers of commercial items strive to ensure that products are safe to use and "fail safe" when they malfunction. Vendors accept responsibility for their products and "certify" their use by private consumers by means of a guarantee. However, this does not mean that systems constructed from commercial parts will, by the vendor guarantees, be certified as "mission ready." There is nothing inherent in the Acquisition Reform approach that ensures that the risk in using commercially based military systems is known, understood, and minimized. The assurance that a vendor will replace a product that fails under normal use cannot be taken as confidence that the product can be depended upon in combat. Commercial vendors strive to make their products dependable for their intended use, but no commercial vendor can be held liable for products bought by the federal government and used in warfare. Any approach used to acquire products for use in warfare must acknowledge the federal government's sole responsibility to ensure the public trust. The successful application of Acquisition Reform requires that a core technical process be established that leads to commercially based systems that are certified for use in warfare.

Certifying the behavior of a system means that the risk in using it has been qualified. Qualifying risk requires the following:

- Defining system risk criteria
- Verifying the system meets the definition
- Testifying to the fidelity of the verification

The first, defining risk criteria, means specifying an acceptable requirement or standard that can be measured. The second, verification, means determining that design data and test data are accurate and consistent with the documented standard. The third, testifying, means the human act of attesting by report, letter, or other means that the system has met the standard within specified limits. The act of certifying includes the acceptance of accountability and liability for the deployed system and responsibility for the certification process, including the standard criteria used. Certification may include a statement of known capability and limitations.

3.0 RISK DEFINITION AND QUALIFICATION

The acquisition process requires "risk management" to control cost and schedule and ensure success in meeting procurement milestones. Procurement "risk" is controlled by an administrative process. Throughout this report, the term "risk" applies to physical events that are controlled in the core technical process.

As previously defined, a computer automated system is a machine consisting of two or more physically and functionally related parts that are interconnected and convert input to output. If a malfunction occurs somewhere in the system, then the system may fail by providing an incorrect output or no output. Also, if the system contains moving parts powered by electrical, mechanical, or chemical energy, then a malfunction could cause the system to damage itself or injure or kill those operating it. The risk in using any system is that it may fail to operate as expected. Military systems are expected to meet an operational requirement and are used to support the accomplishment of a specific mission. The risk in using a system in warfare is the risk that the mission may not be accomplished if the system fails to operate as expected. If the system "fails safe" then it may be possible to restore it to proper operation and still accomplish the mission. If the system cannot be quickly restored, or the failure results in a hazard, the mission may fail. It follows that ***the risk in using a system in warfare is that failure of the system to work as expected may lead to failure to accomplish the mission***. The consequence of this risk is the possibility of a hazard caused by the failed system itself and the prospect of loss of life and property by enemy (or friendly) action due to the mission having failed.

Qualifying the risk of using computer automated systems in warfare involves complex and interrelated issues. Risk assessment is predicated on failure. It must be assumed that all systems can and will fail.

- Hardware components will wear out and fail due to material defects and age.
- Computer programs will have faults due to the huge number of sequences that are possible.

In addition to these failure modes, complex systems may also have design defects that escape the most careful development process and appear unexpectedly after the system is deployed. And, cause and effect relationships are not always completely understood, so fixes may not have addressed the true cause of the defect. Computer programs used in deployed systems contain so many interrelationships that defects are likely to be found during use. Most computer programs undergo almost continuous improvement, and this insidious nature of software requires fault tolerant designs and diligent quality assurance.

The consequence of a failure occurring somewhere within a system is that it may lead to a safety hazard or result in mission negation. The issue of safety will be discussed first since it is also

important in the nonoperational activities of system development, testing, and training. The more complex problem of mission negation will be addressed second.

3.1 SAFETY RISK

A system that suffers a malfunction while operating may present a safety hazard. For example, an electrical short that results in a fire or a software design flaw or implementation defect that causes a control computer to send the wrong signal resulting in either unintended action or lack of intended action. The severity of the safety hazard and the probability that it will occur defines the risk in using the system. Hazard severity is typically described as shown in Table 1. The probability, or frequency of occurrence, of a malfunction leading to a hazard may range from frequent to improbable. Ideally, probability and severity would appear as shown notionally in Figure 2. It should be kept in mind that, for weapons and particularly nuclear weapons, there are severity levels above catastrophic if the effects of detonated warheads are included. It should also be kept in mind that a system does not have to malfunction to present a safety hazard. For example, most radars present a microwave radiation hazard to people. And weapon systems are dangerous by their nature and their design requires that methodical consideration be given to the safety of operators and bystanders.

TABLE 1. HAZARD SEVERITY

Hazard Severity	**Effect on People**	**Effect on System**
Negligible	No injury	No Damage
Marginal	Minor injury	Minor Damage
Critical	Severe injury	Major Damage
Catastrophic	Death	Destruction

Methods for evaluating and managing system safety are well known [4, 5]. The process begins with the first steps in design, and a disciplined analysis is conducted throughout the development. Many safety issues are straightforward, such as use of toxic materials and proper electrical grounding. The latter is different for shipboard applications in that ships do not enjoy the earth ground for which most commercial systems are designed. Safety analysis may lead to design changes to eliminate or reduce the possibility of hazards. Any part of a system that has the potential of becoming a hazard is considered a safety critical part. These safety critical parts should be identified, and attention given to preventing accidents. Military systems are inherently dangerous and rigorous operator training is necessary to prevent accidents. Weapon systems by their very nature will have components that are safety critical and, where possible, these components should be isolated from the rest of the system to prevent malfunctions that occur in parts that are not safety critical from feeding through to parts that are safety critical.

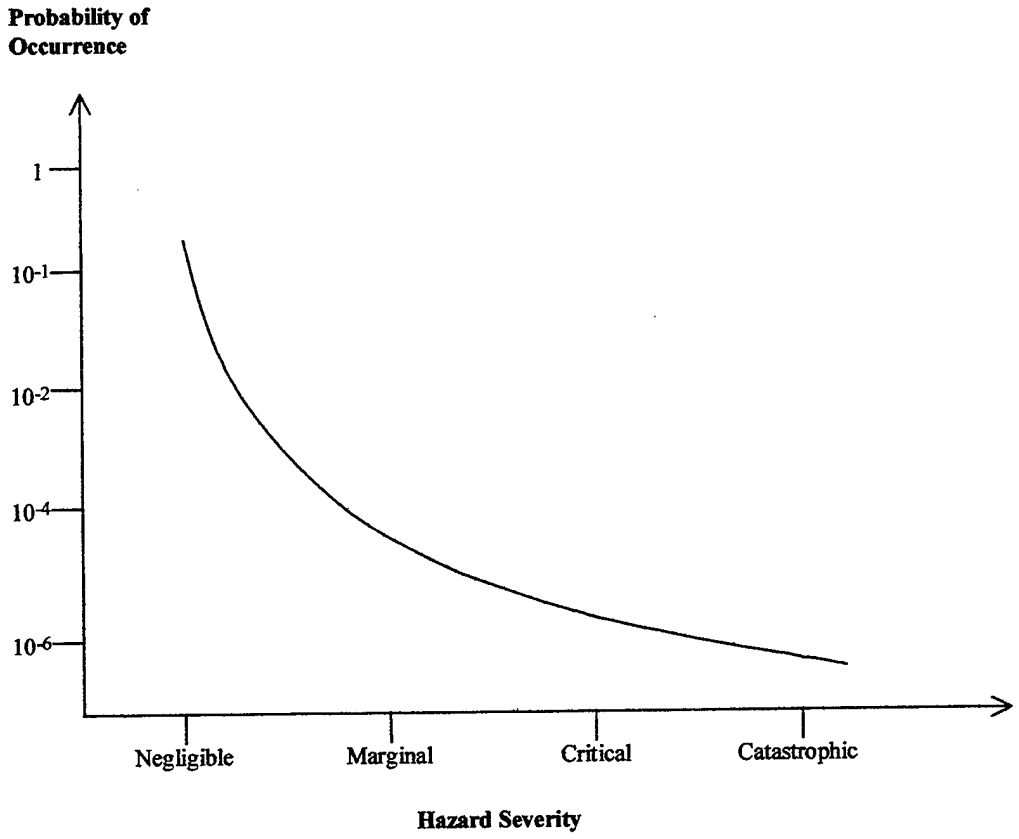


FIGURE 2. HAZARD SEVERITY VERSUS PROBABILITY OF OCCURRENCE (NOTIONAL CURVE)

An example of weapon system safety design is the way engagement orders are handled by the Aegis Weapon System in the AN/UYK-43 baselines. Air target tracks are managed in the system by assigning them track numbers. The Command and Decision computer manages all tracks and is used to initiate an engagement. When an operator orders an engagement of a designated track, a message to engage a specific track is sent from the Command and Decision computer to the Weapon Control computer, which in turn prepares a missile to be launched to intercept the designated track. The safety question that arose was "What if a software fault caused the wrong track number to be specified by the computers?" To reduce the possibility of firing at the wrong target, the engage order sent to the Weapon Control computer is repeated back to the Command and Decision computer for verification. If both computers do not get the same answer twice, the engagement is aborted. As a final measure, the operator can abort the engagement after the missile is launched by sending a microwave signal from the ship to the missile causing the warhead to explode before reaching the target. This design approach accomplished the following three things.

- It reduced the possibility of engaging the wrong target.
- It made everyone involved—civilian engineers and sailors—aware of the potential danger of engaging the wrong target.
- It gave the operators confidence in using the system.

This example was used to illustrate a safety issue. However, there are mission aspects as well. A system used in warfare that malfunctions in a way that leads to engaging the wrong target could lead to mission failure. In general, any safety problem suggests a mission problem as well.

3.2 MISSION RISK

This discussion of mission risk assumes that the hazard severity is negligible as listed Table 1. If success of a mission depends on a given system, then that system must be available and reliable; when called upon it must work and work as expected. Mission risk is determined by availability, reliability, and maintainability of those systems that are depended upon to accomplish the mission. Mission risk is determined by how resilient the system is to malfunctions and by how long it takes to correct a malfunction and restore the system. Mission risk must also include the relationship of the system to the mission. Systems have traditionally been placed in two categories: mission critical and not mission critical. For example, for surface combatants, mobility is mission critical, but an automated bridge for steerage and engine control is not considered mission critical if a manual backup is provided. Weapon systems are typically identified as mission critical since manual backup is impossible. Mission critical systems receive more attention to detail than those that are not mission critical.

Traditionally, mission critical systems had to meet more stringent requirements, cost more, and as a result, systems designated as mission critical were held to a minimum. As systems become more integrated and complex, the line between critical and not critical becomes blurred. Time is a key factor in mission criticality. For example, a Tomahawk mission may take an hour or more to execute so that 10 minutes spent in correcting a malfunction may not affect the outcome of the mission. But, in contrast, an air defense mission may last only a few minutes, and there may be no time available to correct malfunctions. Thus, systems may be equally mission critical but have different requirements for availability and for time to repair. To evaluate mission risk, three questions about the system and its parts must be answered.

- What effect would failure have on the mission?
- How often can failure be expected?
- How long does it take to restore the system after a failure?

Analysis to answer these questions begins with the concept of operation of the system and continues as the system design progresses through production and delivery.

Mission risk analysis should be done for the system in the context of the ship and an acceptable value for the probability of mission failure determined. The greater the potential loss, the smaller the desired probability of incurring it, so that,

$$\text{Probability of mission failure } (P_M) \sim 1/\text{value of the loss.}$$

The potential loss could vary from minor damage to the ship to major damage and casualties and ultimately to loss of the ship with impact on the mission of the deployed force. It must be kept in mind that the cause of mission failure discussed here is due to system malfunction and not to enemy action. A system malfunction that increases vulnerability to enemy action due to mission failure can lead to potential loss. In some cases it may be possible to restore a failed system

fasteners prevented the 17,000 ton *Iwo Jima* from performing its mission. Attention to detail is a key ingredient in qualifying risk and ensuring that systems work as expected.

This example also illustrates how illusive certification can be. The incorrect nuts and bolts that were used clearly satisfied form, fit, and function and thus appeared to be valid replacement parts. When installed, the fasteners were seen to be consistent with the system design. But they were not consistent with the elevated temperature and pressure environment in which the system was intended to operate. Form, fit, and function must be satisfied in the intended operating environment.

In this example the system did not fail due to a defect in the original design but due to a defect that was introduced during maintenance, which illustrates that risk qualification is not a one time event but continues throughout the life of the system. The original certification has to be preserved, and system maintenance and repair procedures included as part of the overall risk qualification process. Computer programs are insidious in this regard as they can and do contain latent defects—"bugs" that may be represented by only one or two bits in programs containing millions of bits. Some "bugs" will be of little consequence while others may have serious side effects. "Bugs" will be triggered by a unique combination of events and occur unpredictably during tests and during routine use of the system. Once found they can be eliminated by changes to the computer program. Unlike the *Iwo Jima* example, maintenance of the computer program does not rely on spare parts but requires continuously available support to diagnose and eliminate faults to preserve certification.

4.0 TRADITIONAL CERTIFICATION PROCESS

"Certification" is often incorrectly assumed to be the final test or inspection of something followed by the act of declaring it "certified." In reality, the act of certifying is the final step of a complex engineering and management process. The traditional process of approving products and systems as ready for Fleet use meant that there was confidence that the product or system would meet prescribed criteria. The required confidence was gained by developing standards and continuously measuring products against them. This involved, for example,

- Design and requirements documentation.
- Change control.
- Qualification testing.
- Engineering analysis and assessment.
- Qualified risk of failure.

Establishing confidence meant that the product's behavior was consistent. Knowledge of system behavior was derived from understanding its internal workings and from multilevel test and analysis. Availability, reliability, and maintainability were quantified, and confidence in the system ultimately led to approval for Fleet use.

The process of creating certifiable products, that is, the certification process, was established and institutionalized over the decades following World War II. A tier 0 illustration of this traditional acquisition process is shown in Figure 3. The controls that were established to maintain the process are listed in Table 2. This list is by no means exhaustive, but it identifies the key controls that defined the prescribed criteria and the process that ensured the acquired products met those criteria.

The process shown in Figure 3 provided two things. The first was a system delivered to the Fleet. The second was repeat production of system parts that were used to build follow-on copies of the system and for spares to sustain the delivered system. The parts included hardware in the form of least replaceable units (LRUs) and computer programs (CPs). The controls over the process (Table 2) ensured that the LRUs that were used to sustain the system were identical to those that the system was constructed from, which ensured that the original certification of the complete system was not invalidated by routine maintenance. In most cases, LRUs were not elements of the system. Elements of the system generally consisted of several LRUs integrated together to form a unit that was interfaced with other elements to form an integrated system. LRUs were stockpiled in numbers consistent with the expected usage rate so that failed and damaged ones could be replaced aboard ship as routine maintenance. The nature of CPs required them to be sustained by a logistics process different than LRUs.

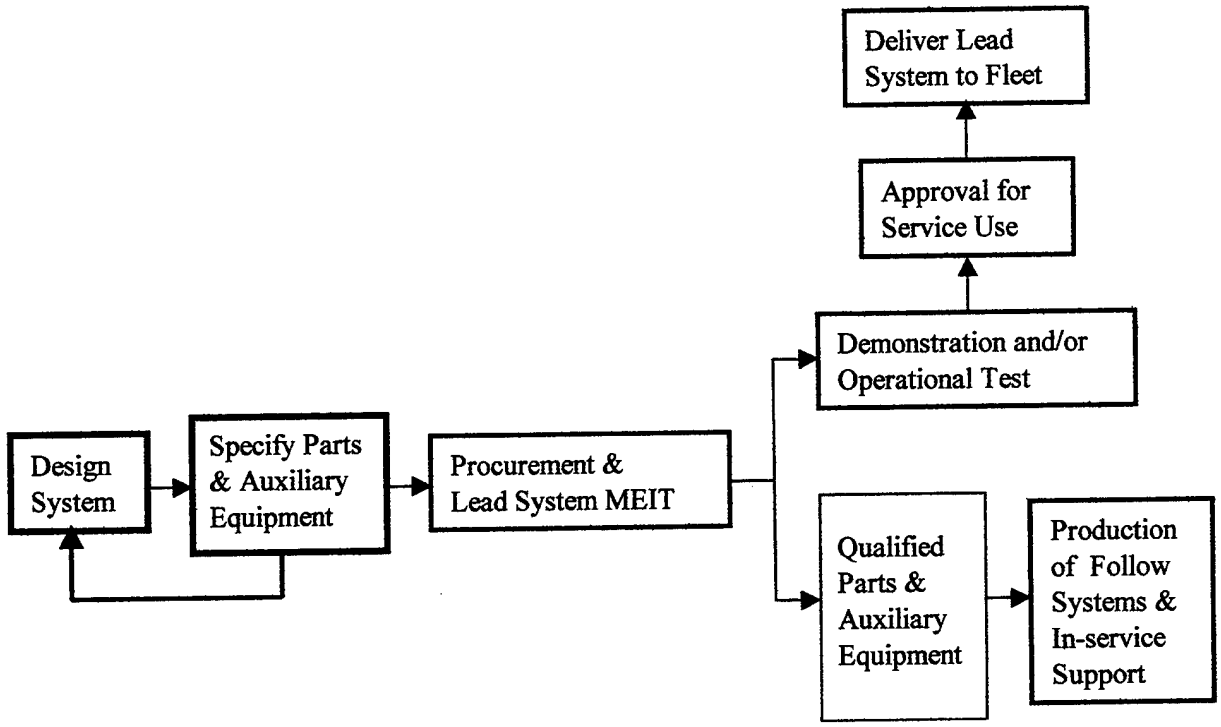


FIGURE 3. TRADITIONAL SYSTEM DEVELOPMENT AND PRODUCTION PROCESS

TABLE 2. TRADITIONAL ACQUISITION PROCESS CONTROL

Qualified Product Lines
Software Qualified with GFI/GFE
Full Change Control
Full Disclosure and Traceability
Rigorous Product Testing
Operational Requirements
Military Standards
Security Classification
Military Specifications
Military Review Boards
Analysis

The routine replacement of CPs aboard ship was done for one of two reasons:

- An error was found in the deployed program.
- An existing function was changed.

Replacement was made by installing new computer programs, or by installing "patches" to existing shipboard programs. Corrections to firmware required replacing the defective component aboard ship with a new one. A different approach was used when there was a change to one or more system elements. This was a conjunctive change of hardware and software and required repeating some or all of the Multi-element Integration and Test (MEIT) process to ensure compatibility of LRUs and CPs and to recertify the system. For this traditional approach, CPs were not stockpiled as LRUs were. Rather, CPs were "built" as needed from source code. Replacement CPs were built using equipment identical to that used in their original development and, before delivery, they were qualification tested on computers identical to the ones that were used in the shipboard system. By this process, changes to CPs were verified and the original certification of the complete system was not invalidated. The traditional approach allowed LRUs and CPs to be maintained independently at different facilities, although in the actual system aboard ship they were interdependent. System development and maintenance were coupled together in such a way that the system was continually certified.

Acquisition of traditional systems required a major effort in technology, engineering, and management. The core technical process that created certifiable systems depended on control of physical risk factors that could affect performance, safety, maintenance, and training. Controlling risk meant that internal failure modes and their effects on system behavior had to be qualified. For example, understanding the risk to the system of the failure of a given LRU required understanding two things:

- Possible failure modes of the LRU, and
- The role of the LRU in the system.

Both required detailed knowledge of the LRU design and the system design. If the LRU is a ***black box***, that is, its internal design is invisible and unknown, then predicting its failure modes is impossible. If the LRU is a black box, then its functions will not be visible, its role in the system cannot be completely understood, and the risk of it failing becomes difficult to predict. The function of the system is the collective function of its LRUs, so that the use of one or more black box LRUs results in the system becoming a black box. That is, if some of the parts of the system are not completely understood, then the system itself cannot be completely understood. The end result in using black boxes is that the severity of the safety hazard and the probability of mission failure become very difficult to predict or control. The traditional process rejected the use of black boxes and required design disclosure that included LRU components and software. This design disclosure was used for two purposes.

- Predict and control risk, and
- Configuration control.

Predicting risk was necessary to certifying the system, and controlling its configuration was necessary to maintaining that certification.

Consistency was a mainstay of the traditional certification process; repeat production was used to ensure interchangeability of parts and consistency of system behavior. Consistency existed within systems, but attempts to establish consistency across systems succeeded only on a small scale. Independent funding lines were established for the different systems so that, although the

overall process was the same, the LRUs and CPs used in different systems varied in detail. For traditional systems, interchangeability in the horizontal sense was limited by configuration control in the vertical sense. The result was that system certification was tailored to each system and consistency across systems was reflected in the use of common military standards and military specifications. The inability to standardize at the LRU and CP level across systems constrained interoperability.

5.0 ACQUISITION REFORM SYSTEM DEVELOPMENT

Adapting the traditional core technical process to one that depends on commercial business practice poses a challenge. The next generation of military systems is expected to be composed of parts purchased from the private sector [10]. The recommended approach is that commercial products not be modified to satisfy system needs but that system requirements, architecture, and design are to be traded off so that commercial products can be used off-the-shelf [11]. For most Navy systems there are some requirements that cannot be satisfied by commercial products. For example, neither 5in/54 gun barrels nor Standard Missile midcourse guidance computer programs are available commercially. Systems developed under the Acquisition Reform approach will consist of commercial parts (modified or unmodified) and Navy parts integrated together. Commercial products may be changed or discontinued in response to sales and competition in the open market place. Thus, commercial parts for maintenance of the system and production of follow-on copies of the system may not be the same as those used in design and construction of the lead system. It will be necessary to continually trade off system requirements, architecture, and design to accommodate changes in the characteristics of the commercial parts. It may also be necessary to modify the Navy unique parts as well to make them compatible with the commercial parts. The end result is that systems that are built at the rate of a few per year may all be different and, once put into service, maintenance may continue to change each one in a different way as spare parts are acquired over time. For such systems, the risk to the user may be neither known nor understood.

The overall definition, design, and development of the system is traded off against available commercial parts. Product selection requires a detailed market analysis to trade off requirements and design so that the use of unique parts can be minimized. The system is built by the Multi-Element Integration and Test (MEIT) process that combines all the system parts and demonstrates the functional—input-output—behavior of the complete system. Following MEIT, the system can undergo additional testing before it is approved for shipboard use. Success in developing the system will depend on the tradeoffs made in the commercial product selection process. The tradeoff process requires that system performance (which includes availability and reliability) become a function of the selected products, and the realizable performance may be different than the initial desired performance.

A system integrated with commercial parts will have a specific configuration determined by the tradeoffs made in the parts selection and design process. The lifetime of commercial products varies and can be as short as 18 months. Given this volatility of available parts, the specific configuration of a system will be time dependent. In general, repeat production will not be possible. Indeed, every copy of the system may differ in detail from every other copy. Also,

system support requires that replacement parts be available for the lifetime of the system. This problem of rapidly changing characteristics of commercial products is frequently referred to as "technology refresh." This continual introduction of "fresh" products to replace discontinued ones leads to difficulty in development, production, and support of military systems. Some form of replanning and reengineering will be ongoing throughout the life of the system [12] leading to incremental, time dependent differences among all copies of the same system. Unless disciplined engineering and management steps are taken to minimize configuration differences, the system may become an aberration to the operators who are expected to rely on it.

Cost has been a major factor in the transition to the reform approach. The life cycle cost of the traditional approach has been viewed as prohibitive. The traditional approach is characterized as one in which performance is the independent variable and cost is the dependent variable. The reform approach advocates the converse; cost is the independent variable. The traditional concept is to expend funds to develop parts, integrate them into an initial system, and establish a production line to produce copies of follow-on systems and spares. The cost curve for this approach is shown notionally in Figure 4. The reform approach is to reduce initial development and production costs by buying commercial parts and integrating them into a system, thus benefiting, at no cost, from the development and production of the private sector. Although expenditures are still required for system integration, the overall cost of the initial system is obviously less than for the traditional approach. Unfortunately, this initial system cannot be put into production at no cost, and integration may have to be repeated for the production of each follow-on system since there will be changes in follow-on generations of off-the-shelf commercial products. The cost curve for this approach is also shown notionally in Figure 4. The reform approach clearly avoids much of the system development and production costs at the expense of almost continuous system design and integration. The reform approach clearly changes the quality assurance challenge from the traditional "build it right the first time and then make identical copies" to the reform "built it right every time."

There is stark contrast between the traditional and the reform paradigms. Exploring these differences will guide the way to finding a new core technical process. The differences between the two that are key to developing and supporting certifiable systems are listed in Table 3 and explained as follows.

- Both the traditional and the reform paradigms rely on MEIT to establish the system; that is, to verify the overall function of the system and to qualify the parts—LRUs and CPs—as true parts of the system.*

- Typically, the design details of commercial products are held as proprietary to prevent disclosure to competitors. Using proprietary products in military systems means that those parts of the system must be treated as black boxes. Failure analysis regarding these parts will require perfecting new and different techniques, or design disclosure must be negotiated with the producer.

* The Government Accounting Office recommended against legislation to reduce test and evaluation, because it " . . . would undermine a key management control . . . " and " . . . test and evaluation should increase, not decrease . . . " (Testimony, 03/22/94, GAO/T-NSIAD-94-124).

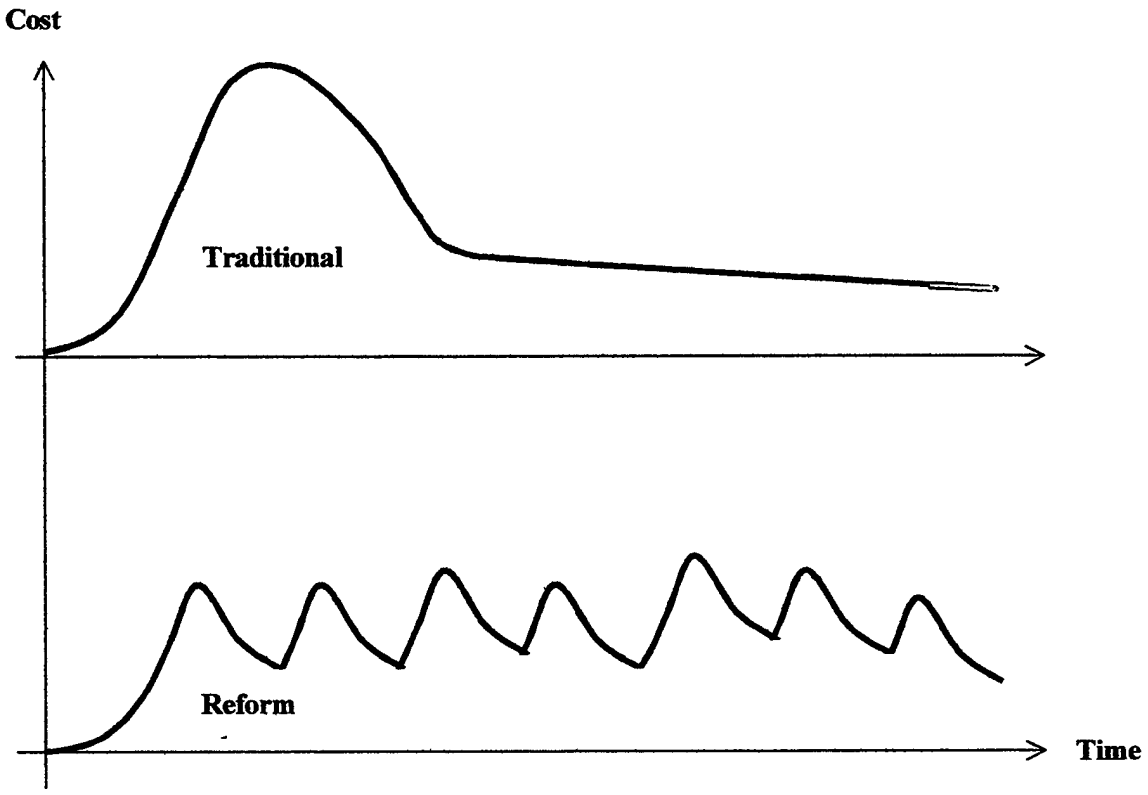


FIGURE 4. TRADITIONAL AND REFORM LIFE CYCLE COST (NOTIONAL CURVES)

TABLE 3. ACQUISITION PARADIGMS

Traditional	Reform
MEIT Established System	MEIT Established System
Design Disclosure of Parts	Proprietary Design of Parts
Repeat Production of Parts	Aperiodic Change of Parts
System Configuration Controlled	System Configuration Managed
System Requirements Specified	System Requirements Compromised

- Once system development is completed, repeat production of parts allows for a supply of identical parts for repeat production of the system and for spare parts. Commercial products frequently change in detail design as well as overall characteristics. Since there is no supply of identical system parts, system development becomes a continuing task and MEIT will be repeated to reestablish the system.

- Configuration control means preserving the identity of the system by requiring replacement parts to be the same as the parts they replaced and by allowing only preplanned changes. Proprietary design and aperiodic changes make configuration control difficult or impossible. However, the configuration can be managed by keeping a detailed record of current parts and specific characteristics of the system over its lifetime.

- Specifying requirements of a system necessarily specifies its parts. If parts are bought off-the-shelf, then their characteristics may not exactly match those required to satisfy predefined system requirements. And if the parts cannot be modified, then the predefined system requirements will have to be changed. If replacement parts differ from the original parts, then the system requirements must again be changed so that development requires compromising predefined requirements, and support may require continuing compromise.

Given these general characteristics of the reform process, it is evident that traditional system certification is no longer viable. Efforts to cope with the reform process continue to evolve and the need for certification has been identified [13]. However, the characteristics of traditional shipboard systems—risk to the user is known, understood, and minimized—cannot be forfeited. The extent to which these characteristics can be achieved will now be discussed.

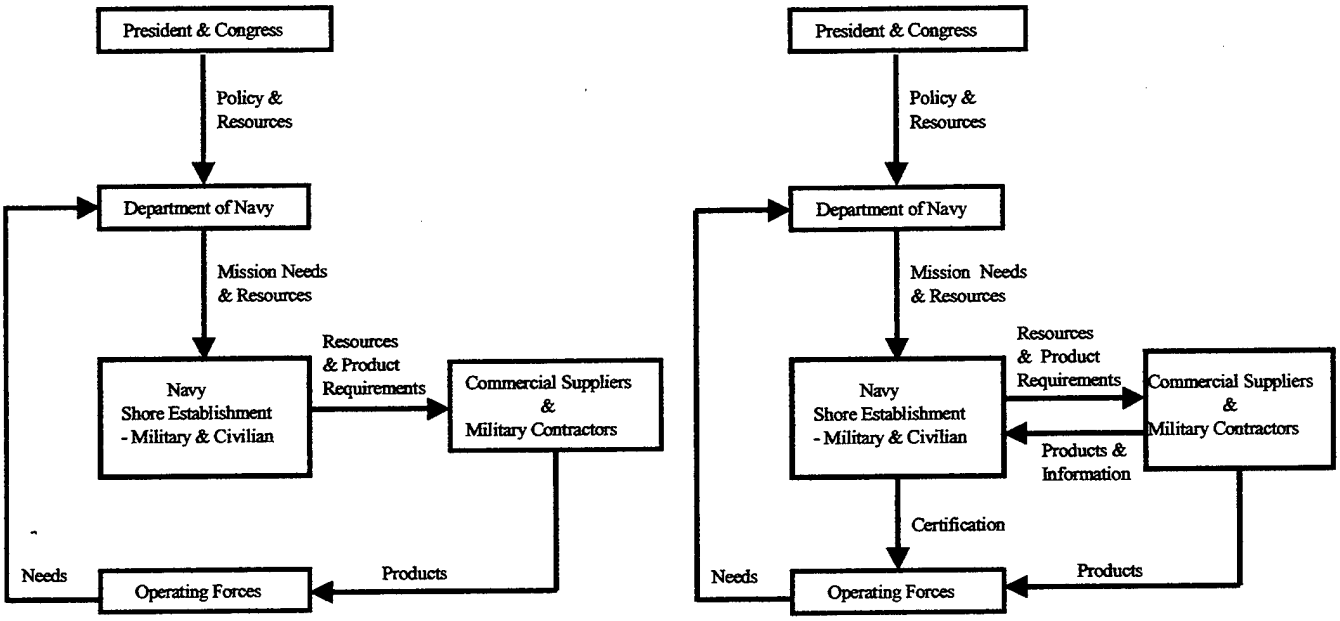
6.0 SYSTEM CERTIFICATION

Systems developed and supported by traditional methods were certified as a consequence of the process as described in previous sections of this report. Traditional engineering is no longer viable, and there is no common procedure available to the various system program offices in the Navy. A new process should be defined and institutionalized so that all systems will benefit equally. The approach taken here is to use the most fundamental factors of certification as a basis for reinventing engineering and management for the core technical process. Figure 5 provides two different interpretations of the reform process. Figure 5a represents an "open loop" interpretation wherein products are delivered directly to the customer bypassing the shore establishment. This interpretation decouples requirements from products and prevents certification by the Navy and places all liability on private industry. This approach may offer advantages for acquiring products requiring warrantee or guarantee but not for systems requiring certification. The "open loop" interpretation will not be discussed further. Figure 5b reflects a coupling of requirements with the product and thus "closes" the certification loop and places the burden of liability on the Government where it must necessarily be. Not shown in Figure 5b is that the certification recipient is the commanding officer of the ship receiving the system. The certification itself should explicitly identify any known limitations of the system. For example, a certification could state that the system has no known faults or that it may not function properly under certain specified operating conditions. And the statement that a system is not well understood or may be unsafe and should not be operated is a de facto certification.

Certification reflects knowledge of the system and how it is maintained. The act of certification implicitly states that:

- The intended use of the system is understood.
- The environment the system will operate in is known.
- The system design is consistent with the operating environment and intended use.
- The system was implemented consistent with its design.
- The capabilities and limitations of the system implementation are known.
- The maintenance process will preserve the design implementation.
- Design changes (even the most minor ones) will require recertification.
- The system was properly installed aboard ship.
- The ship's crew has correct and sufficient information to operate and maintain the system at sea.

Referring again to Figure 5b, the engineering and management process must provide sufficient information for the Navy to validate the nine items listed above and discussed below. It is thus necessary to develop an acquisition plan that ensures validation.



a. Open Loop Process

b. Closed Loop Process

FIGURE 5. TOP LEVEL PROCESS

The intended use of the system is understood. This requires a comprehensive description of the system performance, its mission, and how it will be operated and by whom. Here "performance" is taken in its most general meaning; a detailed description of the way in which the system functions when in use. "Performance" includes such things as operational envelope, safety, availability, reliability, and maintainability. Intended use of the system is nothing less than Government furnished information specifying the desired product.

The environment the system will operate in is known. Here "environment" includes natural conditions such as heat, moisture, and vibration as well as the effects of other shipboard systems and people that the desired system must be compatible with. This requires that the desired system be analyzed, not in isolation but embedded in the natural and manmade environment it is to be operated in. Products from this analysis include some performance specifications and a Test and Evaluation Master Plan.

The system design is consistent with the operating environment and intended use. This evaluation consists of an analysis to determine if the design has taken into account all the performance requirements and the influence of the operating environment. This analysis requires that the design agent furnished information that can be used by the Navy to review and verify that the design satisfies the need. In cases of technical difficulty or high cost, it may be necessary to relax performance requirements to achieve a valid design. A key part of design analysis is evaluating risk as discussed in Section 3.

The system was implemented consistent with its design. Implementation validation should proceed in parallel with the implementation so that validation can be done in manageable steps and corrective action taken when necessary. Implementation is not a replica of the design but rather a synthesis of physical things that represents the design, so validation cannot be achieved by direct comparison of the real with the abstract. On the contrary, it is necessary to determine if the implementation satisfies the intent of the design, including performance and risk as discussed in Section 3. Typically, more than one implementation will be possible, so tradeoff analysis will be required to select the best approach. Establishing and validating an optimum implementation requires an intense technical effort and diligent management.

The capabilities and limitations of the system implementation are known. Predicting the behavior of a system *a priori* is generally not possible since it depends on how the implementation is optimized. It is important to establish the "as built" characteristics of the system and demonstrate its performance in its operating environment. A Navy Test and Evaluation Master Plan is key to evaluating the operational behavior of the system prior to approval for Fleet use.

The maintenance process will preserve the design implementation. Maintenance philosophy is part of the system performance requirement. Details of the maintenance process should be established during design implementation. Shipboard maintenance will involve replacing parts of the system identified as LRUs and possibly by repairing LRUs. Computer program maintenance requires a shore facility to find software faults, fix them, and deliver newly corrected programs to ships. The procedures used for maintenance are based on the requirement that the operational behavior of the system can be sustained at sea.

Design changes (even the most minor ones) will require recertification. The philosophy for operation and maintenance must be based on preserving the design of the system. The "as built" system is a specific configuration of specific parts approved for Fleet use. Any change to the configuration or parts introduces an unknown that could cause the system to behave differently than its certified behavior.

The system was properly installed aboard ship. Prior to deploying, the ship's commanding officer needs assurance that systems have been properly installed and are functional. The shore establishment that is responsible for delivering a specific system to the ship must supervise the system installation and checkout. For small systems, the process may take only a few hours, while for complex integrated systems, it may take many days. In the case of external communication links, installation may involve checking ship-to-ship connectivity.

The ship's crew has correct and sufficient information and training to operate and maintain the system at sea. Operation and maintenance of the system requires that crewmen be "certified" by approved training. This requires that documents and procedures used by the crew accurately reflect the system design, system implementation, and system operation and maintenance philosophy. This requires the Navy to deliver both shipboard and classroom documentation proven to meet the needs of the ship's crew.

To sustain the core technical process, it is crucial that all nine of these implicit factors be recognized and continuously ensured. Dedicated and diligent management is critical to success since these factors can appear as impediments to schedule and cost demands. In reality they are the opposite. Compromising these factors to achieve short term goals can lead to serious consequence. One examples of compromise is the readiness of USS *Hue City* (CG 66) and USS *Vicksburg* (CG 69) to deploy.* Another example is the catastrophic accident aboard the space shuttle Challenger. Both these examples were the result of induced instability of the core technical process. The reasons for the Challenger accident are multiple and have been documented, but they boil down to a failure of the safety certification process. Evaluation of the Challenger core technical process and its products uncovered safety hazards in both the solid rockets and the liquid fuel engine, while the computer system was determined to be of the highest quality. The report of this evaluation [14] offers a fundamental perspective on the meaning of certification and the roles of management and engineering in the core technical process.

6.1 THE NEED FOR STANDARDS

Certification is only valid if referenced to a standard. Standards are the foundation of industry, trade and commerce and have been in use since biblical times. Standards provide measures of comparison for quantitative or qualitative value; criterion that defines a specific condition of a commodity or human behavior. The traditional certification process used Military Standards as discussed in section 4.0. These traditional standards where developed specifically for the purpose of procuring and using products in the military environment. Products that met identified Military Standards were de facto certified. Standards used for commercial products generally were not considered adequate for products intended for use in combat. Military standards were needed to describe the operating environment. Military Standards were also created to support design implementation and define methods for production and testing.

The proliferation of standards during the past century lead to two independent sets—one used to procure military products and one used for commercial products. The two sets had both similarities and differences. For example, the standards required for components used in the 600 psi steam plant of the USS *Iwo Jima* (section 3.3) were similar to the standards for components used in commercial 600 psi steam plants. The existence of an equivalent commercial standard makes the use of a separate military standard difficult to justify. However, real and important differences exist. For example, the anticipated shock and vibration environment for warships is more sever than for commercial vessels. Thus, a Military Standard is required for shock and vibration regardless of the availability of a lesser standard for commercial products. However, the most striking difference in commercial and military standards is purpose. Commercial standards are necessary to facilitate commerce and are driven by the market place. Military standards are driven by the need to ensure deployed systems work as expected. Military standards, in general, do not facilitate commerce and are thus viewed as impeding reform.

* Premature installation of equipment and computer programs on these ships degraded their readiness and prevented either ship from deploying. Rework to make these ships mission ready took over a year.

As part of Acquisition Reform, the defense standardization program was established to minimize the use of government unique specifications. Since 1994 thousands of standards and specifications have been canceled and thousands of others inactivated*. Some Military Standards have been replaced by commercial standards issued by the Institute of Electronic and Electrical Engineers (IEEE), the Standards Engineering Society (SES), and the American National Standards Institute (ANSI). Some Military Standards have been converted to handbooks for standard practice for management. For example, the system safety standard has evolved into a standard practice to be chosen by contractors as need [15].

Certifying the behavior of a system means that the risk in using it has been qualified against a known, valid, documented standard that accurately defines the environment the system is to operate in. In addition, standards for testing and analysis must be applied rigorously**. The study reported here did not include a detailed investigated of specific requirements for certification standards for shipboard systems. The adequacy of the present residue of Military Standards and available commercial standards to support shipboard system certification was not determined as part of the study reported here.

6.2 ROLE OF TEST AND ANALYSIS

Testing of system parts and the complete system is necessary but not sufficient to fully qualify the system. Full qualification requires analysis of design data and data from tests of system parts and the complete system, provided the data is of adequate fidelity. Confidence to qualify a system is developed over time by an accumulation of analysis of design data and test data. The process of system development can be understood in terms of three stages as shown in Figure 6. The process starts with system level requirements such a Mission Needs Statement followed by lower level and more specific requirements that guide the design down to the point of identifying system parts. The process is then reversed for implementation as integration and test proceeds upward from the parts level to the element level until the complete system is created and operationally tested.† In reality this description is idealized in that the actual process is not a continuous smooth flow, but interruptive, iterative, and heuristic as technical, management, and budget problems appear and are resolved. The end result of this requirements-design-integrate-test process is a system consisting of a complex of integrated parts.

---

* See the Defense Standardization Program web page at http://dsp.dla.mil/

** On September 23, 1999 a NASA probe, the Mars Climate Orbiter, failed to enter a stable orbit and apparently crashed into the planet by mistake. A contributor to this failure was later found to be confusion over the standard unit of measure—English or metric—that was used for navigation.

† The Government Accounting Office concluded that this process is successfully being followed by the leading commercial firms they visited but not by the DoD (Chapter Report, 07/31/2000, GAO/NSIAD-00-199).

The system design begins with high level requirements and, as the design progresses in detail, the requirements expand in detail to include LRU components. The test and integration process starts at the lowest level of detail—components of the LRU—and progresses upward to the final integration and test of the complete system. This approach of top down requirements and design followed by bottom up design implementation is holistic in the sense that the system as a whole is defined and the system parts can be viewed in the context of the whole. It also provides the best cost effective results because the implementation proceeds in small steps so that design flaws can be isolated and the cost of fixing them will be contained. The solid line shown in Figure 6 separates two engineering and management domains that do management and engineering. To the right of the solid line is the domain of the Navy and military contractors. To the left of the solid line is the domain of commercial suppliers. The two domains have historically been independent. The requirements and design-integration-test data used to develop and produce commercial products typically stay within the commercial domain. Thus, design data and test data, unless disclosed to the Navy by the commercial suppliers, will be incomplete and analysis of the system will be deficient. So what impact does this analysis deficiency have on qualifying the system so it can be certified? The answer to this question depends upon qualifying risk. If risk can be qualified to an acceptable level, then there is no impact on certifying the system. If not, then approving the system for Fleet use may be imprudent.

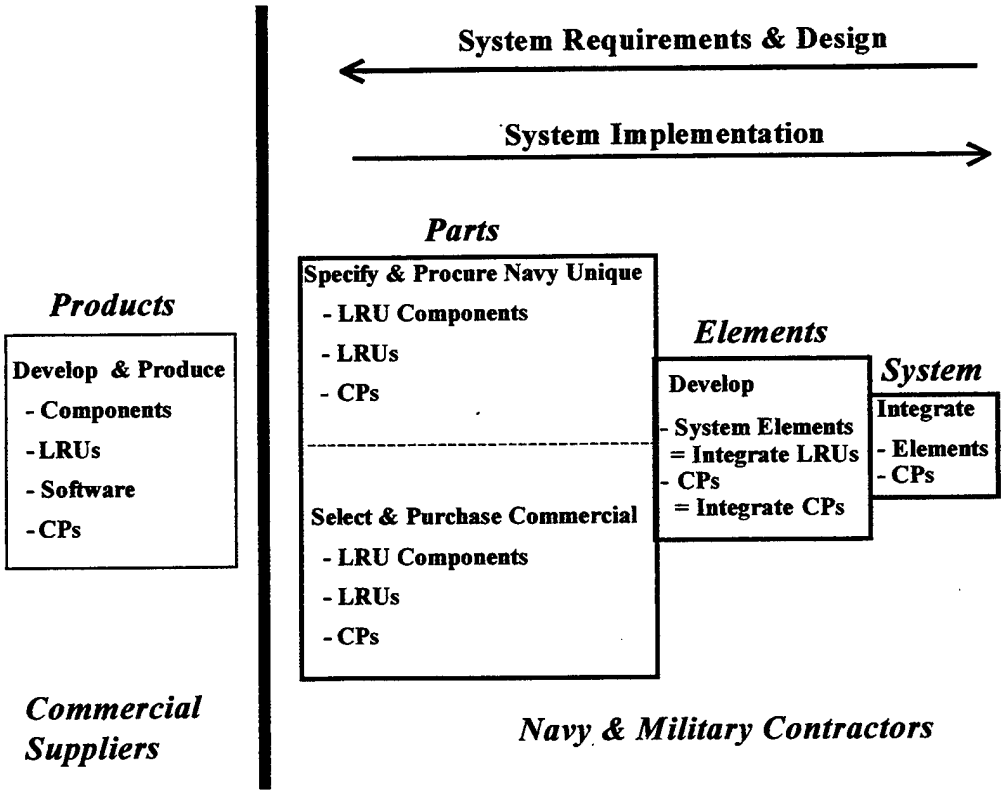


FIGURE 6. STEPS IN SYSTEM DEVELOPMENT

Qualifying risk in using a system, as explained in Section 3, depends on several interrelated factors. The case at hand—a system containing nondisclosed commercial parts—is the classic "black box" problem. To illustrate this problem, consider Figure 7, which represents a hypothetical system consisting of four networked elements. Three of the four system elements are white boxes indicating that their internal workings are known. The fourth element is a black box indicating that its internal workings are unknown. To qualify risk it is necessary to perform an analysis for each element to determine possible failure modes, possible causes of failure, possible effects of failures, probability of occurrence, and criticality. The basis for this analysis is design data for each element, such as functional drawings, schematics, and failure rates of components. Since there is no design disclosure for the black box, it must be treated as single device that converts input to output in an unknown way. The criticality of this element to the system and the effect of its failure on the system can be analyzed, but the failure modes, possible causes of failure, and probably of occurrence are difficult to determine. The element could be tested to determine the variance in output versus test conditions such as temperature, vibration, input variance and so on. This approach is typically how the probability of failure of components such as transistors is determined. However, the black box contains multiple components that must be treated in the aggregate, as a single, very complicated component. It will be necessary to test several copies of the black box, which will introduce yet another variable; that is, box-to-box variance due to component tolerance and the manufacturing process. The primary requirement in testing is to get a large enough sample to ensure stationary statistics. Confidence in test results requires a tradeoff between how many samples are needed and how many samples can be collected [16].

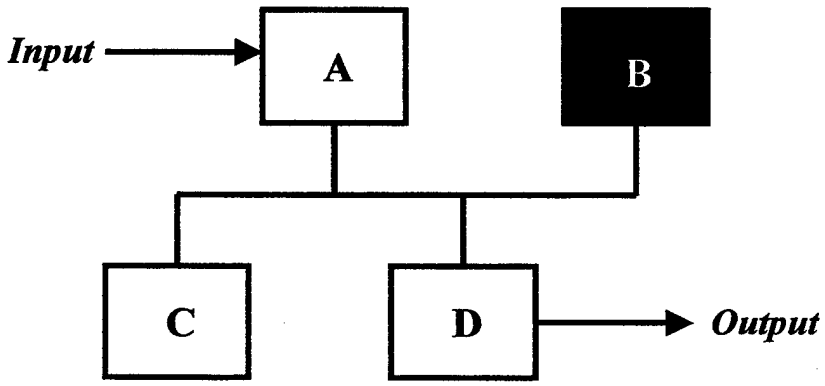


FIGURE 7. HYPOTHETICAL SYSTEM

6.3 IMPACT OF ARCHITECTURE

Systems consist of two or more interacting parts that convert input to output. For the purpose of this discussion, system architecture is a description of the physical relationship of the parts and how the parts functionally interact. Unfortunately this view of architecture is complex since it involves both hardware and software. Hardware contributes to system architecture, for example, by how memory is accessed, by how I/O is supported, and by how independent processors are interrelated. Software contributes to architecture by how the operating system works and by how the application programs relate to each other and to the processors. When the system is

operational, the hardware and software components interact in real time so that, in this view, system architecture is not static but dynamic and includes time dependency of functional relationships of the system parts. System architecture can be complex and the more complex it is the more difficult it will be to certify.

Architectural complexity will be determined by how the system is designed and how the design is implemented. The number of processors and how they are interconnected is an important factor. The simpler the interconnection, the simpler it will be to analyze and test. Redundancy leads to complexity. For example, a system consisting of N parallel, identical, and redundant elements will have 2^N modes of operation including the degenerate one when all N processors fail. Each mode will in fact represent a different implementation of the system and will require test and analysis to validate its behavior. If the same system used nonidentical elements, then analysis and testing would become even more difficult. Thus, design implementations can be simplified by limiting redundancy and maximizing commonality. Limiting redundancy will limit the number of different modes of the system requiring certification. Maximizing commonality will simplify the system configuration, minimize documentation and analysis, and reduce the required test environment. On the other hand, redundancy may be necessary to achieve availability requirements and dissimilar processors may be needed to support different types of functions. Thus, architecture, requirements, and certification are inseparably related.

A large part of the system architecture is determined by the operating system and how it manages resources and interfaces with the application programs. Operating systems and the systems they are hosted on fall in two categories—real time and non real time. Control systems are real time systems; data processing systems are not real time systems. Control systems are required to process specific tasks at specific times so that responses are neither early nor late but periodic. Non real time systems are used to process aperiodic tasks such as graphical user interface. Windows is a commercial operating system that can be used to "run" a variety of non real time application programs such as WordPerfect. VxWorks is an example of a commercial real time operating system. Most traditional weapon systems such as Aegis and Fleet Ballistic Missile are real time systems. The architectural differences of real time and non real time systems are as follows.

- In real time systems, tasks "own" the hardware resources and the operating system is designed to manage the resources (processors, memory, I/O) and support task execution. Task priority is determined by the tasks and stored in an operating system queue. These operating systems are relative small; VxWorks requires about 0.80 MB of memory to install.

- In non real time systems the operating system "owns" the resources and is designed to service tasks. Task priority is determined by the operating system, which also manages the system resources (processors, memory, I/O). These operating systems are relatively large; Windows requires 100 MB or more of memory to install.

Large operating systems pose a quality assurance challenge due to their shear size. Test and analysis to eliminate faults in operating systems such as Windows or UNIX would be a monumental task. Small, agile, real time operating systems could be easily quality controlled and system certification achieved. The current AN/UYK-43 based Aegis Weapon System that

uses a 0.250 MB operating system has been fully certified. Aegis and other shipboard systems require real time operation for only part of the tasks they perform. Most use graphic interfaces and require other tasks that are not real time. Such systems are combinations of real time and not real time tasks that complicate the architecture. Collectively, the operating system and application programs represent the software architecture for the system. Selection of the correct operating system is critical to successful implementation of a system. Much of the overall behavior of a system is determined by the operating system, and knowledge of its internal workings is critical to qualifying risk in using the system.

6.4 ROADBLOCKS

The use of unmodified commercial products in shipboard systems introduces roadblocks to qualifying risk to the user and thus prevents establishing and maintaining certification. Organization and acquisition are the two major roadblocks to smooth transitioning to a new core technical process.

6.4.1 Organizational Roadblocks

The current naval shore establishment evolved with the traditional acquisition process. A significant organization feature is functional segregation that resulted from the fact that LRUs used for maintenance were identical to those that were used to construct the system and that CPs were built and maintained using equipment identical to that used in their original development and used aboard ship. This identity of parts was one aspect of controlling the traditional acquisition process as discussed in Section 4. This approach allowed the functions of development, production, and logistics to be segregated and shore facilities tended to have limited charters and rarely provided full service for shipboard systems. Under the traditional approach, the engineering facilities of the shore establishment evolved into organizations that could specialize in the different stages of the process, thus improving the overall efficiency. The reform approach is inconsistent with this infrastructure.

Figures 8 shows the key steps in the traditional approach to development, production, and support. The system proceeds from design to procurement and MEIT of the lead system, which results in two things: (1) a production model of the system that can be evaluated and, (2) establishment of a production line for the parts of the system and auxiliary equipment needed to produce and support it. Following approval for Fleet use, the production lines provide products for MEIT of follow-on copies of the system. These production lines also provide spare parts and auxiliary equipment for support (maintenance and repair) of the systems that are in service use. Configuration management of a qualified product line allowed software support to be independent of hardware support except when changes to hardware were required. This functional independence led to organizational independence of the hardware and software support functions.

A new approach is shown in Figure 9 that is derived from Figure 8 by introducing the Acquisition Reform requirement to use commercial products to the extent possible. System

design will include a market survey of commercial vendors to determine product performance and availability. If commercial items are selected, this survey will continue throughout the life of the system to assess the availability of the commercial items. Decision points are required to deal with obsolescent and changing commercial items. The first, as shown in Figure 9, is the decision for procurement and MEIT of the lead system. Changes in availability of one or more selected commercial items at this point means that the system cannot be implemented consistent with its design (see Section 6.0) and the design must be revisited. The decision to produce follow-on systems depends on the continued availability of commercial items identical to those used in the lead system. If obsolescence or changes have occurred, then the design of the lead system cannot be implemented in follow-on systems and redesign will be required. Once the system is in use, maintenance and repair will require qualified commercial items. Again obsolescence or changes will require the design to be revisited since parts substitutions may not preserve the original design implementation.

In comparing Figures 8 and 9, Figure 8 represents a linear process that proceeds in steps left to right with each stage (development, production, support) leading to the next. Figure 9 represents a nonlinear process, and inputs can cause the process to reset. The development stage can reset before completion, production can be terminated and development restarted, and maintenance can trigger redesign and restart of the development stage. Figure 9 represents a process in which the development stage sustains both the production and support stages. In Figure 8, the three stages are serial and can be managed independently, but in Figure 9, production and support cannot be managed independent of development. Also, Figure 8 represents a closed process isolated from outside events whereas Figure 9 illustrates an open process that can be influenced by external events—changes in the commercial market place—that can trigger instability. Overcoming these organizational roadblocks requires the following:

- Integrating the roles of development, production, and support
- Buffering external inputs to the process by controlling the rate of obsolescence and change of commercial items

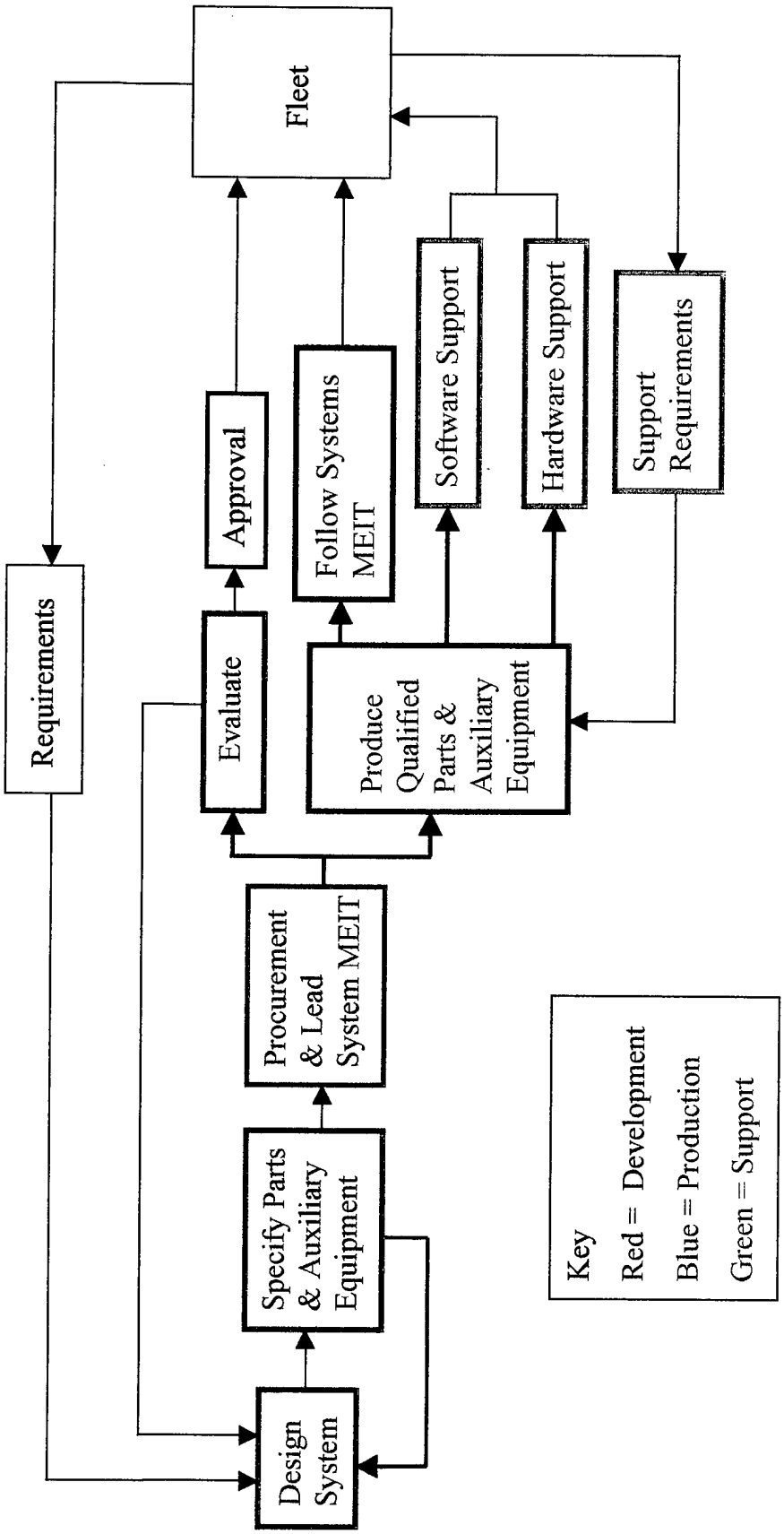


FIGURE 8. TRADITIONAL DEVELOPMENT-PRODUCTION-SUPPORT MODEL

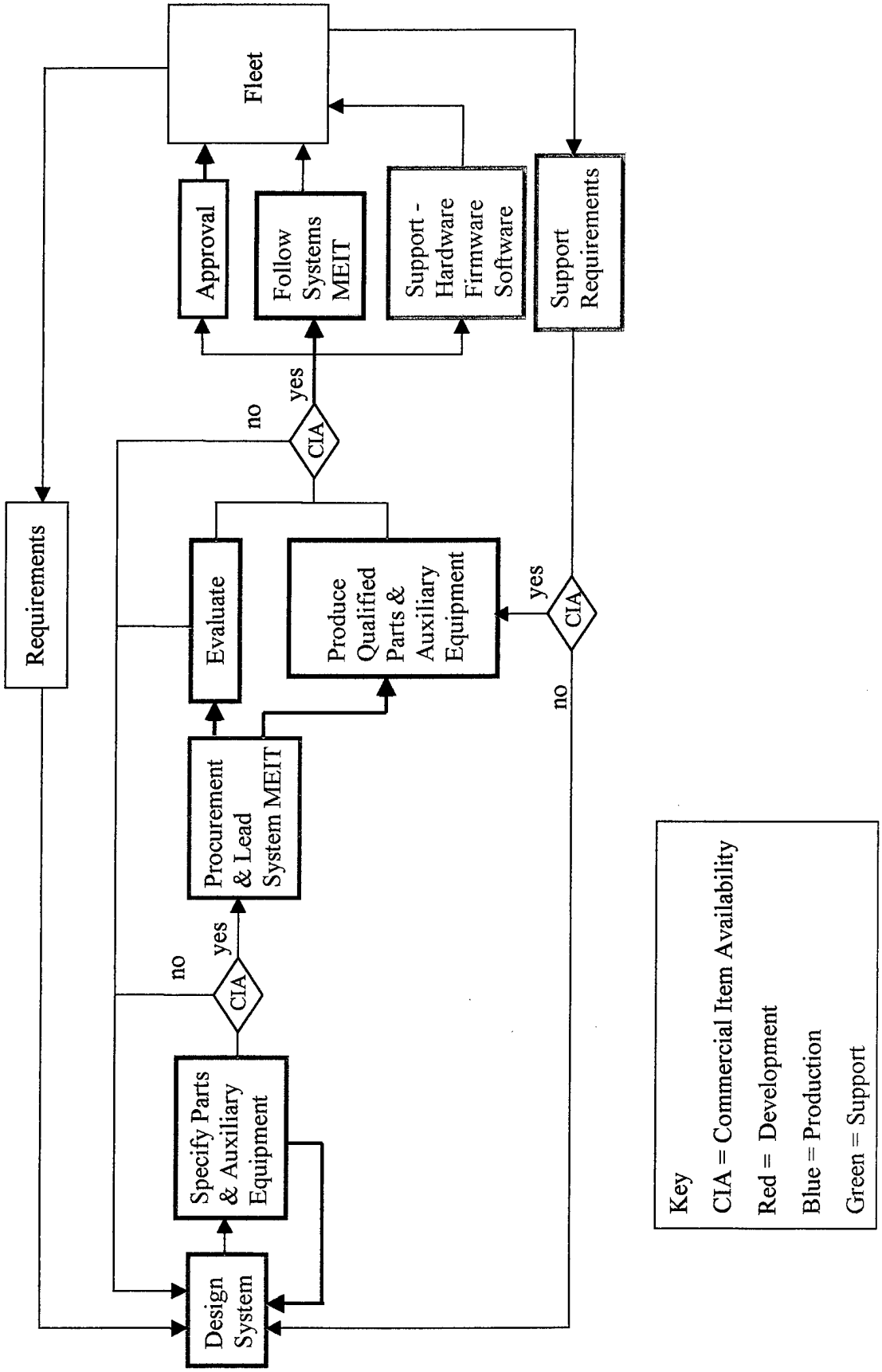


FIGURE 9. NEW DEVELOPMENT-PRODUCTION-SUPPORT MODEL

6.4.2 Acquisition Roadblocks

Short lifetime, nondisclosed commercial products present special problems in engineering and managing the new core technical process, and both are roadblocks to qualifying risk.

Product Lifetime vs. System Lifetime. Large complex systems require several years from concept to service use and significant upgrades to existing systems such as Aegis may take as long as five years. Once approved for service use, many systems will be deployed for 10 years or more. Some commercial products such as automobiles and aircraft are also in use for years and are supported by parts manufactured over long time periods. In contrast, commercial digital electronics and software tend to change on a one- to two-year basis and most are held as proprietary and are only minimally supported. Systems that have long lifetimes and use commercial products that are supported over several years may be certifiable based on historical performance and the consistency of their commercial parts. However, systems that have long lifetimes and use commercial products that have short lifetimes and limited support may be difficult to certify due to uncertainties in their design and configuration.

If the components used to implement a design are changed after the implementation is verified, it will be necessary to reverify the implementation. Repeat production of the system becomes difficult, and each copy may require individual design implementation verification. Also, spares used to support the system may be different than the original parts; thus the maintenance process may not preserve the design implementation. The result of using short lifetime commercial products in systems that are produced over time is that all copies of the same system may not be the same and routine maintenance may introduce more changes over the useful life of the system. As a result, each copy of the system must be treated as potentially unique. For example, if the system is to be deployed on N ships, then it may be necessary to provide life cycle support for N variants of one system and each variant would have its own certification that would be updated as part of the routine maintenance process. Also, variations in the system may require variations in operator training. In addition, the current process for a Battle Group workup before deployment requires 30 months before a 6 months deployment. If this D-30 process exceeds the lifetime of some system components, then there will be additional complications in certifying that ships are ready to deploy. The use of short lifetime commercial products will not prevent certifying systems as mission ready, but the process may lack confidence and may require operators to accept more risk and uncertainty.

Nondisclosure vs. Disclosure. Commercial products are held as proprietary to prevent disclosure to competitors so that design data and source code is generally not available to the Navy for system risk analysis. Specific knowledge of commercial products used in systems is necessary to determine if the system was implemented consistent with its design and to determine the capabilities and limitations of the implementation. Currently there is no practical method that will allow the Navy to accept and protect proprietary data for commercial products. Unless data rights are available to the Navy, it will be necessary to deploy systems containing nondisclosed products—black boxes. Testing of commercial parts both in and out of the system will reduce the amount of disclosure required. Testing can be used to determine input-output

7.0 LEGISLATION AND THE PUBLIC TRUST

The legislative responsibility of the core technical process is manifest in the fact that the recipient of the act of certification is the commanding officer of a ship. The government is ultimately responsible to its people for the actions of military commanders and for the systems they use; certifying shipboard systems is an integral part of acquiring them, and the government is accountable for ensuring that the material elements of an afloat command are mission ready.

The Oath of Office taken by all commissioned officers* is to "defend the Constitution of the United States." And, under the Constitution, a naval officer must comply with regulations issued by the Secretary of the Navy that cover all aspects of naval service. Of particular interest are the following sections of the Navy Regulations [17].

- Section 0702: "Commanders shall be responsible . . . for the satisfactory accomplishment of the mission and duties assigned to their command . . ."
- Section 0704: "Commanders shall take all practicable steps to maintain their commands in a state of readiness to perform their missions."
- Section 0802: "The responsibility of the commanding officer for his or her command is absolute . . . responsibility for the safety, well-being, and efficiency of the entire command."

These Navy Regulations are provided for under Title 10, U. S. Code, Section 6011. The U.S. Code consists of Acts of Congress that represent the will of the American people. Thus, the public provides the commander of a warship the absolute responsibility for readiness, mission accomplishment, and the safety of his or her entire command. Responsibility is ***absolute*** in that it cannot be delegated. Failure to comply with Navy Regulations can result in removal from command and possible court martial as set for under the Uniform Code of Justice, Title 10, Chapter 47.

Making a commander absolutely responsible for readiness, mission accomplishment, and safety means that the ship and shipboard systems must be capable of working as expected. No commander could legitimately be made responsible for the maintenance and operation of a

* As required by law (U.S. Code, Title 5, Section 3331, *Oath of Office*), the same oath must be signed (Standard Form 61, *Appointment Affidavits)* by all individuals accepting appointments to the civil service.

poorly constructed ship outfitted with defective and unsafe systems. The credibility of the Navy Regulations and Congressional Legislation depends on the ship and shipboard systems being fully capable of meeting the expectations of readiness, mission accomplishment, and safety. The public trust bestowed on a commanding officer represents the collective will of all the people and, by virtue of his or her assigned responsibility, the afloat commander is a custodian of the public trust. Public trust in the Congressional Legislation that assigns the commanding officer absolute responsible for maintaining and operating shipboard systems implies that there is also public trust in the quality of those systems. Completeness requires an absolute responsibility for qualifying shipboard systems by certifying to the commanding officer that they are mission ready and will work as expected. The concepts of public trust, responsibility, and qualified systems are interdependent and inseparable.

The need to acquire ships " . . . capable of supporting the Navy's mission from the first day of commissioned service . . . " is expressed by OPNAV Instruction 4700.8H [18]. The purpose of this instruction is to "augment" the U.S. Navy Regulations. It assigns responsibilities to various commands and defines procedures they must follow for the legal act of accepting custody of ships delivered by private contractors. The act of "accepting custody" of the ship by the Navy requires transition from contractual authority to command authority; that is, the Navy's absolute responsibility is established as the contractor's responsibility is brought to an end. The procedure typically takes 18 months and includes a 6 months warranty period following delivery of the ship in which the contractor is held financially liable for failure in performance, workmanship and/or material quality.* The Navy's responsibility is established by a series of "trials" and "inspections" of the ship and all of its systems and subsystems to ensure the ship is complete and to find and correct "construction deficiencies." Following delivery, the ship is commissioned and its warfare systems undergo trials and tests at sea. The ship is then placed in a shipyard to correct deficiencies and make authorized improvements.

The purpose of Instruction 4700.8H is to make sure the complete ship is in good working order by macro "trials" and "inspections" of complete systems; visibility into design is not required. This instruction assigns command responsibility to ensure the Fleet has " . . . complete ships, free from both contractor and government responsible deficiencies." The procedure is intended to uncover operational defects, it is not a substitute for qualifying risk. It provides a ship level certification process and takes advantage of the U.S. Navy Regulations by making commanding officers legally responsible. It defines the apex of the total certification process but does not, nor can, define the lower tier responsibilities and engineering methods that should be used in the core technical process that creates the ship. Command responsibility cannot be extended to the core technical process so long as it requires civilians employed by the Navy and by private companies under contract to the Navy. And responsibility for the core technical process has been further complicated by legislation requiring the participation of commercial vendors. The core technical process is not defined in Instruction 4700.8H. But, the following excerpts taken from paragraph 7g imply that a process to qualify risk is required.

---

* Title 10, Section 2403, requiring major weapon system warranties was repealed in November 1997 following a General Accounting Office report (Chapter Report, 06/28/96, GAO/NSIAD-96-88).

- "All required control equipment, auxiliaries, fittings, electronic equipment, combat system equipment . . . must be operable . . . and must be capable of meeting performance specifications."

- "Certification of sonar, other acoustic processors, combat control systems . . . is required. When . . . requirements exist which cannot be achieved until after delivery, full certification is not required. However, in these cases all other elements of certification will be accomplished and certified prior to Acceptance Testing."

- "Complete test memoranda, reports, and certificates . . . must be available for inspection by the Trial Board."

Current legislation does not appear to provide regulations for assigning responsibility for quality assurance of military systems. The U.S. Code, Title 41 (Public Contracts), Section 425, appears to prohibit requirement of a certification by a contractor. Indeed, private companies that contract for Navy ships and shipboard systems represent not all but only a small fraction of the American people and thus cannot be expected to be custodians of the public trust. The warranties and guarantees typical of products in the commercial sector establish responsibilities and liabilities between and among individuals and groups but they are meaningless in terms of the public trust. The public trust requires absolute responsibility, not avenues for claims under commercial warranties and guarantees that would seek to delegate responsibility. The procurement philosophy for shipboard systems, particularly weapons, should be based on the concept that "all sales are final." Some commercial products are expected to meet stringent standards, but some, such as commercial software, are not. For example, in early 1999 lobbyists for private industry supported Congress in establishing and passing a Y2K liability bill (HR 775) that would limit claims in the private sector resulting from computer failures on or after 1 January 2000.* In contrast, the Chief of Naval Operations, acting on absolute responsibility for his command, established a Y2K Project under Rear Admiral Jay M. Cohen, USN, who in turn issued a Master Test Plan " . . . to assure mission functionality of all operating units . . . " [19]. The concern of the Navy was readiness not liability. This example illustrates how the two domains—commercial and military—responded differently to the same issue even though both relied on Congressional Legislation to define responsibility. The key difference is that shipboard systems, whether they use commercial products or not, should carry with them mission ready certification, not limited liability.

There are mandatory procedures placed on major defense acquisition programs by authority of the Secretary of Defense in accordance with Title 10, U. S. Code. The revision dated January 4, 2001, *Interim Regulation, DoD 5000.2-R*, [20] reflects an acquisition vision of the core technical process. These mandatory requirements are not presented hierarchically; they must all be satisfied simultaneously. A limited review of this document from the perspective of mission ready certification finds the following to be germane.

---

* Many computer programs were thought to contain a design implementation that used only the last two digits of the year and would record 2000 as 00 and thus read the date as changing from 1999 to 1900, wreaking havoc with military systems, government, banks, utilities, and the public infrastructure in general.

- Section 2.9.1.4.2: "The PM [Program Manager] shall work with the user to define and modify, as necessary, requirements to facilitate the use of commercial and non-developmental items." . . . " . . . the PM shall require contractors and subcontractors to use commercial and non-development items to the maximum extent possible." . . . "Preference shall be first to commercial items, then to non-development items."

- Section 5.2.6.4: "The PM shall establish formal software change control processes."

- Section 5.2.8: "The PM shall establish Reliability, Availability, and Maintainability (RAM) activities early in the acquisition cycle. The PM shall develop RAM system requirements . . . and state them in quantifiable, operational terms, measurable during development and operational T&E."

- Section 5.3.2: "If no acceptable, nongovernment standards exist, the Department may define an exact design solution with military specifications and standards, as a last resort, with MDA-approved waiver."

A propensity for commercial items is evident although the traditional need for change control and reliability, availability, and maintainability is clearly stated. But, as discussed previously in this report, neither effective change control nor availability, reliability, and maintainability may be satisfactorily accomplished for commercially based shipboard systems.

Fortunately, Part 3 of the mandatory procedures for PMs—*DoD 5000.2-R*—is the requirement for a Test and Evaluation Master Plan (TEMP). The TEMP and its contents are clearly outlined, suggesting a traditional approach to test and evaluation that specifically includes commercial items. Also, in Section 3.5, "The developing agencies . . . " are required to "Formally certify the system ready for Operational Test and Evaluation (OT&E)." Section 3.6 specifically makes the DoD responsible for OT&E, and Section 3.6.2 limits the role of contractors in the OT&E process. Reliance on a TEMP and the DoD responsibility to execute it should facilitate mission ready certification of shipboard systems. Although T&E is a large part of qualifying risk, OT&E occurring at one point in time is inadequate to ensure availability, reliability, and maintainability over the system lifetime. Control over and visibility into the parts used in the system are necessary to ensure effective change control and reliability, availability, and maintainability over the lifetime of the system. Visibility into commercial items is restricted by the regulations, exceptions, and conditions for visibility into commercial items set forth in the U.S. Code, Title 10, Chapter 137, Section 2320; *Rights in Technical Data.* The mandatory use of commercial items, and their use as black boxes as is implied by the mandatory procedures, will reduce the effectiveness of OT&E as the lone method for certification and, over the life cycle of the system, introduce risk to the user.

8.0 CONCLUSION

Certification as discussed here is a complex and protracted process that ensures the integrity of military systems that must be operated under conditions of qualified risk. There will be milestones in the process where individuals will be required to attest or approve by their signature that certain work has been completed. Examples are requirements documents, test plans and reports, and reports attesting to the validity of implementation of hardware and software. Attesting to the correction of known computer program design flaws is an important duty for computer programmers and the integrity of small parts of the system may be attested to by workers and lower level managers whereas larger system parts will require the signature of higher level managers. Once the system reaches approval for Fleet use its certification will consist of a pyramid of signatures each reflecting an individual's sphere of responsibility. The apex of the pyramid will be the final certifying official for the complete system. The purpose of identifying individuals in the certification pyramid is to establish responsibility, that is, by signing, the employee acknowledges responsibility to the employer and the employer acknowledges responsibility to the Fleet, and the public trust is assured.

The risk in using commercially based military systems can be reduced by a disciplined engineering and management infrastructure. Overcoming acquisition roadblocks to certification is critical to ensuring the public trust. Organizational changes are required within the naval shore establishment to create an infrastructure that can take absolute responsibility for the quality of shipboard systems. New business practices are needed to form teaming arrangements with the shore establishment, military suppliers, and commercial suppliers that can effectively support the absolute responsibility of the shore establishment. Alternative methods for government use of and protection of proprietary products and intellectual property are needed.

Institutionalizing a new core technical process involves management, engineering, and legislative issues. The U.S. code and the DoD acquisition procedure based on it should be reviewed in detail and modified as necessary to ensure certification requirements are supported. The mandated use of commercial items should be replaced with the requirement to adapt commercially developed technology for military use consistent with Congressional policy set forth in Title 10, Section 2501, *National Security Objectives Concerning National Technology and Industrial Base.*

The core technical process should not be used to facilitate legislation; it should be used to apply the principles of physics and engineering in a managed acquisition environment protected by legislation. Mission ready certification of shipboard systems requires dedicated managers and engineers who have faith in the process and products for which they have absolute responsibility. Faith in the process and products of others is not a substitute. The current process will evolve to

align the acquisition vision with technical reality. Ultimately a new core technical process will be institutionalized that is effective in making sure shipboard systems work as expected and are sustainable at sea.

The studies reported here focused on risk qualification and certification for safety critical and mission critical systems; particularly software dependent systems. Systems used ashore for other purposes such as simulation, analysis, or training were not specifically considered. Nor was the use of commercial products in hull and machinery systems such as electrical and piping. The issue of electromagnetic interference was not addressed although it is a growing problem due to the use of commercial communication equipment aboard ship. Work following this study should address certification at the total ship level and encompass hull, machinery, weapons, and communications. Specific standards for certification need to be identified and applied rigorously.

9.0 REFERENCES

1. Simone M. Youngblood, et al., "Simulation Verification, Validation, and Accreditation," *Johns Hopkins APL Technical Digest*, July-September 2000, Vol. 21, Number 3, p. 359.

2. CJCSI 6212.01B, *Interoperability and Supportability of National Security Systems and Information Technology Systems*, 8 May 2000.

3. William Perry, Sec Def memo on *Acquisition Reform*, 15 March 1994.

4. Harold E. Roland and Brian Moriarty, *System Safety Engineering and Management*, John Wiley & Sons, Inc., New York, N.Y., 1990.

5. Michael Zemore, *Weapon System Safety: Bridging the Gap Between Hardware and Software*, NSWCDD/TR-96/217, January 1997.

6. Fulvio E. Oliveto, "Configuring Computer Suites for Performance, Reliability, and Availability—A Systems Approach," *Proceedings of IEE Annual Reliability and Maintainability Symposium*, Philadelphia, Pa., 27-29 January 1981, pp. 310-316.

7. C. F. Barker and C. B. Campbell, "Risk Management in Total Ship Design," *Naval Engineers Journal*, July 2000, p. 355.

8. *Report of the Presidential Commission on the Space Shuttle Challenger Accident (In Compliance with Executive Order 12546 of February 3, 1986)*, Government Printing Office, Washington, D.C., 6 June 1986.

9. David G. Peterson, "Anatomy of a Catastrophic Boiler Accident," *National Board Bulletin*, Summer 1997, p. 21.

10. U.S. Code, Title 10, Section 2377, *Preference for Acquisition of Commercial Items.*

11. Arthur L. Money and J. S. Gansler, letter from the Office of the Secretary of Defense, 14 July 2000.

12. Ed Morris and Cecilia Albert, *Commercial Item Acquisition: Considerations and Lessons Learned*, Software Engineering Institute (SEI), Carnegie Mellon University, 26 June 2000.

REFERENCES (Continued)

13. *Commercial Item/Non-Development Item Management Plan*, July 1999, Department of the Navy, Program Executive Office for Theater Surface Combatants, 2531 Jefferson Davis Highway, Arlington, Va. 22242-5265

14. R. P. Feynman, "Personal Observations on the Reliability of the Shuttle," Appendix F of the *Report of the Presidential Commission on the Space Shuttle Challenger Accident (In Compliance with Executive Order 12546 of February 3, 1986)*, Government Printing Office, Washington, D.C., 6 June 1986.
Also see Richard P. Feynman, *What Do You Care What Other People Think*, Part 2, W. W. Norton & Co, Inc., New York, N.Y., 1988.

15. "MIL-STD-882D, Standard Practice for System Safety, Published February 10", *Defense Standardization Program Journal for the Defense Standardization Program Committee*, Volume 1 Number 1, May/June 2000.

16. For a discussion of this problem and test and evaluation in general see, e.g., Benjamin S. Blanchard, *Logistics Engineering and Management*, *Chapter 8*, Prentice-Hall, Englewood Cliffs, New Jersey, 1974.

17. *United States Navy Regulations 1990.* Issued by H. Lawrence Garrett, III, Secretary of the Navy, Department of the Navy, Washington, D.C.

18. OPNAV Instruction 4700.8H, *Trials, Acceptance, Commissioning, Fitting Out, Shakedown, and Post Shakedown Availability of U.S. Naval Ships Undergoing Construction or Conversion*, OP-321D3, 5 December 1990.

19. *Naval Year 2000 (Y2K) Master Test Plan, Version 3.0*, July 1999, Department of the Navy, Office of the Chief of Naval Operations, 2000 Navy Pentagon, Washington, D.C. 20350-2000.

20. DoD Directive 5000.1, *The Defense Acquisition System* and *DoD Instruction 5000.2, Operation of the Defense Acquisition System.*

DISTRIBUTION

Copies

DOD ACTIVITIES (CONUS)

ATTN VADM GEORGE NANOS 1
COMNAVSEASYSCOM
1333 ISAAC HULL AVENUE SOUTH EAST
WASHINGTON, D.C. 20376

ATTN RADM MICHAEL MATHIS 1
COMNSWC
1333 ISAAC HULL AVENUE SOUTH EAST
WASHINGTON, D.C. 20376

ATTN RADM WILLIAM COBB 1
PEO THEATER SURFACE COMBATANTS
1333 ISAAC HULL AVENUE SOUTH EAST
WASHINGTON, D.C. 20376

ATTN RADM ROBERT BESAL 1
COMOPTEVFOR
7970 DIVEN STREET
NORFOLK VA 23505

ATTN MATTHEW REYNOLDS 1
NAVSEASYSCOM
T&E OFFICE (SEA91T)
1333 ISAAC HULL AVENUE SOUTH EAST
WASHINGTON, D.C. 20376

ATTN NEIL BARON 1
NAVSEASYSCOM
SEA 53C
1333 ISAAC HULL AVENUE SOUTH EAST
WASHINGTON, D.C. 20376

ATTN CODE A76
(TECHNICAL LIBRARY) 1
COMMANDING OFFICER
CSSDD NSWC
6703 W HIGHWAY 98
PANAMA CITY FL 32407-7001

Copies

DEFENSE TECH INFORMATION CTR
8725 JOHN J KINGMAN RD SUITE 0944
FORT BELVOIR VA 22060-6218 2

ATTN JIM SIMMONS 1
SPAWAR SYSTEMS CENTER SAN DIEGO
53560 HULL STREET
SAN DIEGO CA 92152-5001

ATTN RADM CHARLES HAMILTON 1
PEO SURFACE STRIKE
2521 JEFFERSON DAVIS HIGHWAY
ARLINGTON, VA 22202

ATTN RADM ROLAND KNAPP 1
PEO CARRIERS
1333 ISAAC HULL AVENUE SOUTH EAST
WASHINGTON, D.C. 20376

ATTN RADM DENNIS MORRAL 1
PEO EXPEDITIONARY WARFARE
1333 ISAAC HULL AVENUE SOUTH EAST
WASHINGTON, D.C. 20376

ATTN CAPT CHARLES GODDARD 1
PMS 500
2521 JEFFERSON DAVIS HIGHWAY
ARLINGTON, VA 22202

ATTN CAPT JOHN GEARY (PMS 400B) 1
AEGIS PROGRAM OFFICE
1333 ISAAC HULL AVENUE SOUTH EAST
WASHINGTON, D.C. 20376

ATTN PATRICIA DEAN 1
DEPARTMENT 31
NAVAL UNDERSEA WARFARE CENTER
DIVISION NEWPORT
1176 HOWELL STREET
NEWPORT, RI 02841

Copies

NON-DOD ACTIVITIES (CONUS)

THE CNA CORPORATION
P O BOX 16268
ALEXANDRIA VA 22302-0268 1

ATTN CAPT VAUGHN MAHAFFEY 1
EG&G
P O BOX 552
16156 DAHLGREN ROAD
DAHLGREN VA 22448-0552

ATTN DR THOMAS CLARE 1
TAC ASSOCIATES
10100 MULLIGAN COURT
FREDERICKSBURG VA 22408

INTERNAL

B		1
B02	CAIN	1
B60	TECHNICAL LIBRARY	3
C		1
CD22	BECHTEL	1
D		1
G		1
J		1
K		1
T		1
N		1
N04	SHEEHAN	1
N05	PARKER	1
N05	PITTS	1
N10		1
N10	HOLDEN	5
N60	GONZALEZ	1


NAVSEA
DAHLGREN
Surface Warfare Center Division